Algebra és számelmélet gyakorlat
(matematika BSc)
2024/2025 I. félév

2024. November 22.

1. Prímhatvány modulusú kongruenciák

1.1. Feladatok

1. Oldjuk meg az kongruenciát!

$$x^2 + x + 1 \equiv 0 \pmod{49}$$

2. Oldjuk meg a következő kongruenciát!

$$x^2 \equiv 26 \pmod{55}$$

3. Oldjuk meg az kongruenciát!

$$x^2 + 3x + 7 \equiv 0 \pmod{25}$$

4. Oldjuk meg az kongruenciát!

$$x^3 + x + 3 \equiv 0 \pmod{125}$$

5. Oldjuk meg az alábbi kongruenciát úgy, hogy a felírt kongruenciát visszavezetjük prímszámhatvány-modulusú kongruenciákra.

$$3x^2 + 5x - 2 \equiv 0 \pmod{12}$$

2. Rend

2.1. Definíció. *Legyen* $(a, m) = 1$. *A* k *pozitív egészt az* a *rendjének nevezzük modulo* m, *ha* $a^k \equiv 1 \pmod{m}$, *de bármely* $0 < i < k$ *esetén* $a^i \not\equiv 1 \pmod{m}$

Az a rendjét $o_m(a)$-val jelöljük. Például $o_7(2) = 3$, $o_{10}(3) = 4$ stb. Az Euler-Fermat-tételből következik, hogy minden $(a, m) = 1$ esetén létezik az a-nak rendje és $o_m(a) \leq \varphi(m)$.
A rend fogalma csak $(a, m) = 1$ esetén értelmezhető: ha $(a, m) \neq 1$, akkor egyáltalán nem létezik olyan $k > 0$ kitevő, amelyre $a^k \equiv 1 \pmod{m}$ teljesülne.

2.1. Feladatok

1. Határozzuk meg az alábbi rendeket:

   a.) $o_{13}(4)$

   b.) $o_{13}(2)$

   c.) $o_{107}(4)$

   d.) $o_{67}(-3)$

2. Melyik a legkisebb prím, amelyre

   a.) $o_p(2) = 8$

   b.) $o_p(3) = 5$

   c.) $o_p(2) = 6$

2.2. Házi feladat

Oldjuk meg az alábbi másodfokú kongruenciákat!

a)

$$2x^2 + 7x + 4 \equiv 0 \pmod{19}$$

b)

$$x^2 + 2x - 1 \equiv 0 \pmod{7}$$

2.3. Hasznos linkek

modulo m hatványozás
Waldhauser Tamás (YouTube) - Az Euler féle φ függvény